UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/587,727	07/26/2006	Daniel Timmermans	NL040060US1	1413

30868 7590 04/30/2010

KRAMER & AMADO, P.C.
1725 DUKE STREET
SUITE 240
ALEXANDRIA, VA 22314

EXAMINER	
ZIA, SYED	
ART UNIT	PAPER NUMBER
2431	
NOTIFICATION DATE	DELIVERY MODE
04/30/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

clewis@krameramado.com
docketing@krameramado.com
catta@krameramado.com

Office Action Summary	**Application No.** 10/587,727	**Applicant(s)** TIMMERMANS, DANIEL	
	Examiner SYED ZIA	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2010*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 10-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 10-16* is/are rejected.

7)☒ Claim(s) *17-22* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This office action is in response to application filed on January 14, 2010. Claims 1-8, and 10-22 are pending for further consideration.

Allowable Subject Matter

Claims 17-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

Applicant's arguments filed on January 14, 2010 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-8 and 10-16 applicants argued that Vergnes, discloses nothing of circuits 412-1 and 412-2 performing the same function with different logical operations. Applicant submits that disclosing that functions may be the same does not constitute a disclosure that, in addition to the functions being the same, the logical operations are different. The second fact establishing that Vergnes' circuit 412-2, in contrast, does not, and cannot, operate on the same input data as circuit 412-1 because the Vergnes combinatorial circuits 412-1 and 412-2 are in series".

This is not found persuasive. The system of cited prior art teaches a system and method for a processing circuit that is configured to receive an input in order to create an output. The system performs reshaping of current consumption during processing time period by an additional combinatorial circuit, thus reducing the processing period during encryption/decryption to make current analysis more difficult. In this system a controller is coupled to the processing circuit and is configured to track L manipulations, wherein L is an integer. The controller is further configured to send a select signal to the processing circuit and to cause the processing circuit to manipulate the input over N clock cycles. N is an integer and N is less than or equal to L. N varies over the plurality of processing time periods. An output port is coupled to the processing circuit and is configured to convey the output (Fig.4-6, and [0031-0036, 0046-0047, and 0051]).

Thus the system of cited prior art provides a system and method for having a set of combinatorial logical circuits, the set of combinatorial logical circuits comprising a first combinatorial logical circuit, arranged to perform a first set of logical operations on input data and to produce output data, the output data having a functional relation to the input data

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter recited in independent and dependent claims. Accordingly, rejections for claims 1-8, and 10-16 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-8, and 10-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Vergnes (U. S. Publication No.: 2005/0089060 A1).

1. Regarding Claim 1 Vergnes teaches and describes an electronic circuit for cryptographic processing, having a set of combinatorial logical circuits, the set of combinatorial logical circuits comprising a first combinatorial logical circuit, arranged to perform a first set of logical operations on input data and to produce output data, the output data having a functional relation to the input data, characterized in that the set of combinatorial logical circuits further comprises at least a second combinatorial logical circuit, arranged to perform a second set of logical operations on the same input data and to produce output data, the output data having an identical functional relation to the input data, wherein the first set of logical operations is different from the second set of logical operations, and wherein the electronic circuit is arranged to dynamically select one combinatorial logical circuit of the set of combinatorial logical circuits for performing logical operations on the input data and producing output data (Fig.4-6, and [0031-0036, 0046-

0047, and 0051]).

2. Regarding Claim 5 Vergnes teaches and describes an electronic circuit for cryptographic processing, comprising: a combinatorial logical circuit arranged to perform logical operations on input data and to produce output data, a storage element for storing output data produced by the combinatorial logical circuit, characterized in that the electronic circuit further comprises a first set of an encoding means and a corresponding decoding means, arranged for encoding first output data before storing the first output data in the storage element and decoding the first output data after retrieving the first output data from the storage element, respectively, and wherein the electronic circuit is arranged to dynamically control the activation of the first set of an encoding means and a corresponding decoding means (Fig.4-6, and [0031-0036, 0046-0047, and 0051]).

3. Regarding Claim 10 Vergnes teaches and describes a method of processing cryptographic data, comprising: using a set of logical operations for processing input data and producing output data, storing the output data in a storage element, characterized in that the method further comprises: encoding the output data before storing the output data in the storage element, decoding the encoded output data after retrieving from the storage element, dynamically controlling the encoding and corresponding decoding of the output data (Fig.4-6, and [0031-0036, 0046-0047, and 0051]).

4. Regarding Claim 16 Vergnes teaches and describes a method of processing cryptographic data, comprising: generating a mode signal having one of a given plurality of states;
receiving a given input data and generating a cryptographic processed data output, said generating including:
generating a first input data, wherein the first input data is a selected one of a mask of the given input data and a not mask of the given data, the selection based on the state of the mode signal; generating a second input data, wherein the second input data is the other of the mask of the given input data and the not mask of the given data, performing a first set of logical operations on the first input data to generate a first output data, the first set of logical operations embodying a given input-output function, performing a second set of logical operations on the second input data to generate a second output data, the second set of logical operations being different than the first set of logical operations and the second set of logical operations embodying the same given input-output function, and merging the first output data and the second output data to generate the cryptographic data output; repeating said generating a mode signal to have a different one of the given plurality of states; and repeating said receiving a given input data and generating a cryptographic processed data output (Fig.4-6, and [0031-0036, 0046-0047, and 0051]).

5. Claims 2-4, 6-8, and 11-15 are rejected applied as above rejecting Claims 1, and 5. Furthermore, Vergnes teaches and describes a method of processing cryptographic data, wherein

As per Claim 2, comprising at least a first set of combinatorial logical circuits and a second set of combinatorial logical circuits, and arranged to use output data produced by the first set of combinatorial logical circuits as input data of the second set of combinatorial logical circuits (Fig.4, and [0031-0033, and 0051]).

As per Claim 3, further comprising: a selection circuit arranged for generating a signal to select one combinatorial logical circuit of the set of combinatorial logical circuits, a splitter circuit arranged for inputting the input data to one combinatorial logical circuit of the set of combinatorial logical circuits, depending on the signal, a merger circuit arranged for outputting the output data from one combinatorial logical circuit of the set of combinatorial logical circuits, depending on the signal (Fig.4, and [0034-0036, 0046-0047]).

As per Claim 4, further comprising a timing circuit arranged to determine the points in time at which the selection circuit generates the signal to select one combinatorial logical circuit of the set of combinatorial logical circuits (Fig.4-6, and [0046-0048]).

As per Claim 6, further comprising a second set of an encoding means and a corresponding decoding means, arranged for encoding second output data before storing the second output data in the storage element and decoding the second output data after retrieving the second output data from the storage element, respectively, wherein the encoding of the first output data is different from the encoding of the second output data, and wherein the electronic circuit is further arranged to dynamically select one set of an encoding means and a corresponding decoding means, of a set comprising at least the first set of an encoding means and a corresponding decoding means and the second set of an encoding means and a corresponding decoding means, for encoding and decoding of the output data (Fig.5, and [0037-0045]).

As per Claim 7, further comprising a timing circuit arranged to determine the points in time at which the electronic circuit selects one set of an encoding means and a corresponding decoding means, of a set comprising at least the first set of an encoding means and a corresponding decoding means and the second set of an encoding means and a corresponding decoding means (Fig.5, and [0046-0049]).

As per Claim 8, the combinatorial logical circuit comprises a first combinatorial logical circuit and at least a second combinatorial logical circuit, the first combinatorial logical circuit arranged to perform a first set of logical operations on input data and to produce output data, the output data having a functional relation to the input data, the second combinatorial logical circuit arranged to perform a second set of logical operations on the same input data and to produce output data, the output data having an identical functional relation to the input data, wherein the first set of logical operations is different from the second set of logical operations, and wherein the electronic circuit is arranged to dynamically select one combinatorial logical circuit, of a set comprising at least the first combinatorial logical circuit and the second combinatorial logical circuit, for performing logical operations on the input data and producing output data (Fig.4-6, and (Fig.4-6, and [0031-0047, and 0051]).

As per Claim 11, a cryptographic device comprising an electronic circuit according to claim 1 (Fgi.4-6).

As per Claim 12, the selector includes: a first mask circuit for selectively masking and not masking, based on the signal, the given input data for input to the first combinatorial logical circuit, and a second mask circuit for selectively masking and not masking, based on the signal, the given input data for input to the second combinatorial logical circuit (Fig.4-6, and [0031-0036, 0046-0047, and 0051])..

As per Claim 13, the selector includes: a first mask circuit to selectively mask and not mask, based on the signal, the given input data and to input the selected masked and not masked given input data to the first combinatorial logical circuit, and a second mask circuit to selectively mask and not mask, based on the signal, to input the selected masked and not masked given input data to the second combinatorial logical circuit (Fig.4-6, and [0031-0036, 0046-0047, and 0051])..

As per Claim 14, the first mask circuit includes an AND mask configured to mask and to not mask the given input data by inputting to the first combinatorial logical circuit a selection between all zeros and the given input data, respectively and wherein the second mask circuit includes an AND mask configured to mask and to not mask the given input data by inputting to the second combinatorial logical circuit a selection between all zeros and the given input data, respectively (Fig.4-6, and [0031-0036, 0046-0047, and 0051])..

As per Claim 15, the selector includes an OR merger circuit to receive {.he output of the first combinatorial logical circuit and to receive the output of the second combinatorial logic circuit, and to output, as the selected output, a logical OR of the output of the first combinatorial logical circuit and the output of the second combinatorial logic circuit (Fig.4-6, and [0031-0036, 0046-0047, and 0051])..

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
April 16, 2010
/Syed Zia/
Primary Examiner, Art Unit 2431